SAP SuccessFactors ♡

Setting Up SAP SuccessFactors with Identity Authentication and Identity Provisioning Services

THE BEST RUN **SAP**

Content

Change History

Learn about changes to the documentation for setting up SAP SuccessFactors with SAP Cloud Identity Services - Identity Authentication and Identity Provisioning in recent releases.

1H 2021

Type of Change	Description	More Info
Change	This guide has new SAP Branding: • SAP Cloud Identity Services - Identity Authentication service • SAP Cloud Identity Services - Identity Provisioning service	

2H 2020

The following table summarizes changes to this guide for the 2H 2020 Release.

What's New	Description	More Info
November 20, 2020		
Changed	You can use the monitoring tool track the progress of your upgrade.	Monitoring Tool for the Upgrade to SAP Cloud Identity Services - Identity Authentication [page 17]Monitoring Tool for the Upgrade to SAP Cloud Platform Identity Authentication
Changed	Updated information around Dummy email, SendMail, and Password status transformations	Configure Transformations in SAP Cloud Identity Services - Identity Provisioning [page 25]Configure Transformations in Identity Provisioning
Changed	Added information around setting up a default password transformation for nonemail users	Set Up Default Passwords Using Transformations [page 29]Set Up Default Passwords Using Transformations
October 16, 2020		
Changed	We've enhanced the process for upgrading your tenants. When you upgrade, you can select the tenant to upgrade to.	Initiating the Upgrade to SAP Cloud Identity Services - Identity Authentication Service [page 14]Initiating the Upgrade toSAP Cloud Platform Identity Authentication

1 Overview of the SAP SuccessFactors and the SAP Cloud Identity Services - Identity Authentication Service Integration (Video)

The process of migrating to the Identity Authentication service requires you to perform tasks in SAP SuccessFactors *Admin Center*, the Identity Provisioning service Administration Console, and in the Identity Authentication service Administration Console.

Steps to Integrate with Identity Authentication

Integrating your SAP SuccessFactors Suite with the SAP Cloud Identity Services - Identity Authentication service involves the process described, at a high level, in the image. Select an image to find the topics associated with each task.

> → Tip
>
> If your company migrated to the Identity Authentication service, before April 24, 2020, you will need to make changes to your Identity Provisioning Transformations. The changes that you need to make are described in detail in the guide linked below: **IPS Transformations Document**
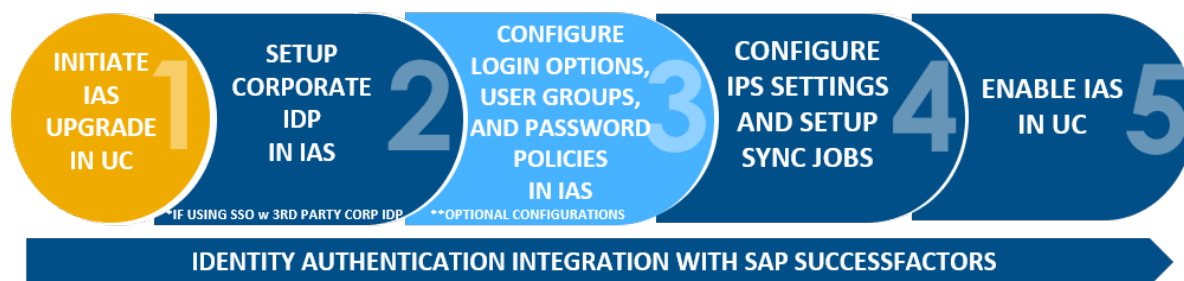
- Initiating the Upgrade to SAP Cloud Identity Services - Identity Authentication Service [page 14]
- Configuring the Corporate Identity Provider in the Identity Authentication service (Video) [page 42]
- SAP Cloud Identity Services - Identity Authentication Service Administration Console Tasks [page 36]
- SAP Cloud Identity Services - Identity Provisioning Service Administration Console Tasks [page 46]
- Testing and Activating the Upgrade to SAP Cloud Identity Services - Identity Authentication [page 22]

Overview of the Identity Authentication Upgrade

Setting Up SAP SuccessFactors with Identity Authentication and Identity Provisioning
Services
**Overview of the SAP SuccessFactors and the SAP Cloud Identity Services - Identity
Authentication Service Integration (Video)**

PUBLIC   **5**

Open this video in a new window

Related Information

IPS Transformations Document↗

Setting Up SAP SuccessFactors with Identity Authentication and Identity Provisioning
Services

**Overview of the SAP SuccessFactors and the SAP Cloud Identity Services - Identity
Authentication Service Integration (Video)**

6   PUBLIC

# 2 Important Notes About Using SAP SuccessFactors with SAP Cloud Identity Services - Identity Authentication

Before you set up your SAP SuccessFactors system to use the SAP Cloud Identity Services - Identity Authentication service, you should be aware of the following notes.

- **Data centers in different regions.** The Identity Authentication service has data centers in various global regions but they are not a one-for-one match with SAP SuccessFactors data centers. During authentication, some personal information is passed between SAP SuccessFactors and the service.
  When an Identity Authentication tenant is assigned to you, you're provided by email with details about your system, including the region of both your SAP SuccessFactors and Identity Authentication tenants.
  If you have any data protection and privacy concerns about the region your tenant is in, contact us to request a tenant in the appropriate region.
- **SAP NS2 exclusion.** For now, SAP SuccessFactors customers using SAP NS2 are excluded from initial migration to the Identity Authentication service.
- **Changes to Company ID.** As with all integrations, the connection to the Identity Authentication service is impacted by a change in Company ID. If you ever need to change the Company ID of your SAP SuccessFactors system, you need to update the configurations in the Identity Authentication service accordingly. For more information, see here ."
- **Data Protection and Privacy.**
  If you use the SAP Cloud Identity Services - Identity Authentication service, be sure to review the latest documentation to ensure that it meets your data protection and privacy requirements. For more information, see here.
- **Global Assignment and Concurrent Employment (GA/CE)** are supported for upgrade to the Identity Authentication service.
- **Integrated External Learners** and **Onboarding 2.0** are supported for upgrade to the Identity Authentication service.
- > ! Restriction
  >
  > After you've upgraded to the Identity Authentication service, you won't have the ability to turn on partial SSO in SAP SuccessFactors company Provisioning. By default, partial SSO is disabled after activating Identity Authentication. If needed, you can set up partial SSO in Identity Authentication.
  >
  > After you've upgraded to the Identity Authentication service, you won't have the ability to enable multiple SAML asserting parties in SAP SuccessFactors company provisioning. By default, Identity Authentication will be enabled as the single SAML asserting party in the SAP SuccessFactors provisioning setting after activating Identity Authentication. If you need multiple asserting parties, you can accomplish this by setting up conditional authentication.
- **Removal of unique email address**: We do **not** recommend that you use the feature that allows you to create a non-unique, null, or blank emails. This feature is not supported by all SAP SuccessFactors product areas so we recommend that you do not use this functionality.
- *SHA-256* is the default hashing algorithm for signing certificates for all integrations. *SHA-1* is **not** recommended as *SHA-256* provides a higher level of security.

Setting Up SAP SuccessFactors with Identity Authentication and Identity Provisioning
Services
**Important Notes About Using SAP SuccessFactors with SAP Cloud Identity Services -
Identity Authentication**

PUBLIC **7**

- When you are onboarding employees and you need to activate those users after you've migrated to the Identity Authentication service, follow the procedure described in **Activating an Account and Setting New Password After Identity Authentication Service is Enabled**. For more information, refer to this topic in Related Information section.

Related Information

Activating an Account and Setting New Password After Identity Authentication Service Is Enabled

Setting Up SAP SuccessFactors with Identity Authentication and Identity Provisioning
Services
**Important Notes About Using SAP SuccessFactors with SAP Cloud Identity Services -
Identity Authentication**

8   PUBLIC

3   SAP SuccessFactors with SAP Cloud Identity Services - Identity Authentication (Video)

All SAP SuccessFactors systems can be set up to use the SAP Cloud Identity Services - Identity Authentication service.

SAP Cloud Identity Services - Identity Authentication service is a cloud solution for identity life-cycle management. It is used by SAP Cloud solutions like the SAP SuccessFactors HXM Suite, as well as for SAP Business Technology Platform applications and on-premise applications. It provides services for authentication, single sign-on, and on-premising integration as well as self-services such as registration or password reset for employees, customer partners, and consumers.

You can use Identity Authentication services like SAML 2.0 single sign-on, username and password login, two-factor authentication, and other login options to control access yourSAP SuccessFactors system.

Step-by-Step Upgrade to Identity Authentication

Open this video in a new window

Related Information

Setting Up SAP SuccessFactors with Identity Authentication and Identity Provisioning Services
SAP SuccessFactors with SAP Cloud Identity Services - Identity Authentication (Video)

PUBLIC   **9**

3.1 Migration to SAP Cloud Identity Services - Identity Authentication Service

All SAP SuccessFactors systems can use the SAP Cloud Identity Services - Identity Authentication service. We plan for all systems to be migrated to the service in the future.

> **i Note**
>
> When your SAP SuccessFactors is connected to the Identity Authentication service, it handles all logins (via password, two-factor authentication, or corporate identity provider) for your SAP SuccessFactors system.

For the latest announcements and migration dates, refer to the Customer Community🌥.

3.2 Benefits of Using SAP Cloud Identity Services - Identity Authentication Service

Here are some of the important benefits of setting up your SAP SuccessFactors system to use the SAP Cloud Identity Services - Identity Authentication service.

- **Connection to other SAP solutions.** Using the Identity Authentication service as an identity provider is the first step to enabling future integrations with other SAP solutions.
- **More login options.** The Identity Authentication service supports username and password login and SAML 2.0 SSO login, just like SAP SuccessFactors does now. It also supports two-factor/token authentication, Social Sign On, SPNEGO, and some Corporate User Stores.
- **More security.** The Identity Authentication service supports SHA-256.
- **Better user experience.** The Identity Authentication service provides a better logon experience than the current SAP SuccessFactors Partial SSO option.
  - No password-specific URL required for first-time login.
  - If user clears cookies, they need to enter email or username again.
- **Conditional Authentication.** You can set up the Identity Authentication service to direct users to either a corporate identity provider or a password login option, based on conditional rules. You can use this feature to replace the current SAP SuccessFactors Partial SSO and Multiple Asserting Party Selection features.
- **Risk-Based Authentication.** You can set up the Identity Authentication service to require different login methods, such as password, two-factor authentication, or Social Sign On, based on risk-based rules.
- **Stand-alone Identity Provider.** As the Identity Authentication service is enhanced, you can use new features.
- **Self-service.** You can access common SSO settings from SAP SuccessFactors *Admin Center* and all other configuration options directly in administration console of your Identity Authentication tenant.

Setting Up SAP SuccessFactors with Identity Authentication and Identity Provisioning
Services
**SAP SuccessFactors with SAP Cloud Identity Services - Identity Authentication
(Video)**

10   PUBLIC

3.3 When to Use SAP SuccessFactors with SAP Cloud Identity Services - Identity Authentication

Determine if you have to set up your SAP SuccessFactors system to use the SAP Cloud Identity Services - Identity Authentication service.

There are three scenarios that require you to set up SAP SuccessFactors with the Identity Authentication service:

- **You want to integrate SAP SuccessFactors with other SAP applications.**
  For example, SAP Cloud Identity Services - Identity Authentication service is a prerequisite for using SAP Analytics Cloud with SAP SuccessFactors. First, you have to set up the connection between SAP SuccessFactors and the Identity Authentication service. Then, you can connect to other dependent SAP applications, like SAP Analytics Cloud.
- **You need additional functionality that SAP SuccessFactors doesn't natively support.**
  Identity Authentication supports much more functionality than SAP SuccessFactors does natively. You want to take advantage of these features.
- **You're a new customer setting up your SAP SuccessFactors system for the first time, but your system was created before Q1 2020.**
  Identity Authentication is the recommended solution for identity management. If you're setting up a new SAP SuccessFactors system, use Identity Authentication from the start to avoid extra migration effort in the future.

> i Note
>
> Starting in the Q1 2020 release, all new SAP SuccessFactors systems are automatically connected to Identity Authentication, so you don't have to set up the integration yourself. We set up the default configuration for you. Then you can use the SAP Cloud Identity Services - Identity Authentication administration console to change the default configuration or enable additional features.

4 Getting Started with Identity Authentication and SAP SuccessFactors

Learn about the overall process to set up your SAP SuccessFactors system and how to use the SAP Cloud Identity Services - Identity Authentication service.

Here is an overview of the process:
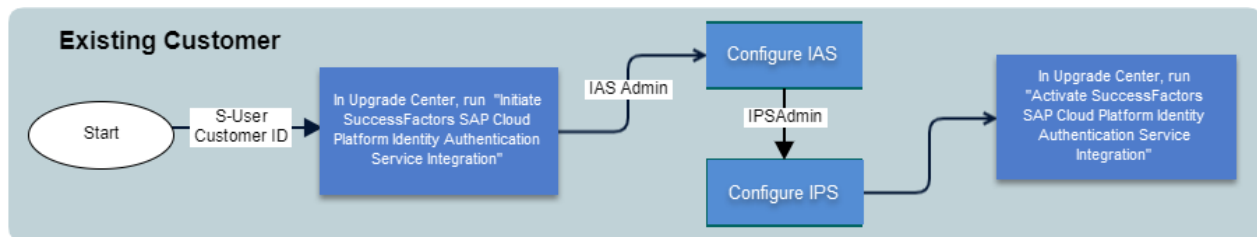
1. **Integrate SAP SuccessFactors with Identity Authentication.**
   - Initiate the process to upgrade your SAP SuccessFactors system using the *Upgrade Center*. You're notified by email when the connection is complete.
2. **Confirm that user sync is set up in the SAP Cloud Identity Services - Identity Provisioning service.**
   - Set up sync jobs with Identity Provisioning service.
   - Ensure that the user that is configured in the Identity Provisioning service *Properties* tab (API User) has the necessary role-based permissions to export user data with OData API.

> ⚠ Caution
>
> You must sync **ALL** users to the Identity Authentication service before you activate the Identity Authentication service. User sync is critical when using the following services and features:
>
> - **Conditional Authentication:** To set up with rules that authenticate based on email, user type, or group.
> - **People Analytics, Internal Career Site, and other SAP SuccessFactors product areas:** User identifiers can change between product areas and the Identity Authentication service can only map these identifiers correctly when your users are in the Identity Authentication service.
> - **Global Assignment & Concurrent Employment:** when users log on from different sources, Identity Authentication service needs to convert their identifiers so that the Identity Authentication service understands them. That only happens when user sync has been done and the users are loaded into the Identity Authentication service.
> - **Enablement of Partial SSO:** If you intend to user partial sso, your users should exist in Identity Authentication service.
> - **Two-factor Authentication:** Your users need to exist in Identity Authentication service so that you can take advantage of two-factor security features.

3. **Review the default configurations.**
   Review the default configuration of Identity Authentication service to determine if it meets your requirements or if additional configuration is required.
4. **Additional configuration optional features.**
   Configuration options in Identity Authentication include:

- Password policy settings
- Single sign-on (SSO)
- Identity Authentication service user groups to configure multiple authentication methods
- Conditional and risk-based authentication rules
- Two-factor authentication
- Email notification templates
- Branding

5. **Turn on the Identity Authentication service.**
   - Enable Identity Authentication in the SAP SuccessFactors *Upgrade Center* after you're finished setting it up.

Related Information

4.1 Default Configuration of Identity Authentication Service with SAP SuccessFactors

When you upgrade to the Identity Authentication Service, your users are configured to authenticate using passwords by default. You can customize these configurations for the needs or your organization.

The Identity Authentication Service is the Identity Provider and performs the user authentication method you configure for your system, session management, and single sign-on for your integrated applications. This integrated process requires the synchronization of users from the SAP SuccessFactors instance to the Identity Authentication Service.

When a new user is created in SAP SuccessFactors, they're provisioned in Identity Authentication and the provisioned user receives an activation email that they can use to set the password that they can use access their SAP SuccessFactors application.

> → Tip
>
> Successfully syncing your users to IAS requires that the SAP SuccessFactors users MUST contain the following attributes:
>
> - Last Name
> - Unique Username
> - Unique Email
>
> These attributes are required in IAS. If you cannot ensure that all users have a unique email address, you may need to generate "dummy" emails for them.

> ⚠ **Caution**
>
> The *sf.user.filter* in the *Identity Provisioning Service Administration (IPS) Console* under the tabs ▌ *Source Systems* ❯ *Properties* ▐ , contains place holder values called, *'sf_username1_placeholder','sf_username2_placeholder'*. Replacing these place holders with a few users can help you to test user provisioning before performing the sync job that pulls in all of your SAP SuccessFactors users into IAS. Test your selected users by substituting the place holders with usernames from your SAP SuccessFactors system. After testing and ensuring that user provisioning is working correctly, remove the placeholder users and replace them with the value `Active`. This syncs all the active users in your system.

Identity Authentication is configured as follows:

- Password-based logins only
- Standard password policy
- Authentication rules configured to send all users to password-based logon
- No user groups configured
- No corporate identity provider (IdP) configured to handle single-sign on

Related Information

Default Configuration of Identity Authentication Service with SAP SuccessFactors [page 13]
Opening the SAP Cloud Identity Services - Identity Authentication Administration Console [page 61]

4.2 Initiating the Upgrade to SAP Cloud Identity Services - Identity Authentication Service

Initiate integration of your organization's SAP SuccessFactors system with the SAP Cloud Identity Services - Identity Authentication service so that you can use it for identity management.

Prerequisites

- You have the SAP *S-User* user name and password.
- You want to be set up as an administrator of your organization's first SAP Cloud Identity Services Identity Authentication service tenant **or** you can gather the required information from the current administrators of your organization's existing SAP Cloud Identity Services Identity Authentication service tenant.
- You have access to theSAP SuccessFactors *Upgrade Center.*

Context

> ⚠ **Caution**
>
> Completing this task initiates the Identity Authentication service upgrade process, after configuring your authentication methods as described in this guide, you must then activate the Identity Authentication service to complete the migration.

Procedure

1. Go to ❙▶ *Admin Center* ❭ *Upgrade Center* ❭ *Optional Upgrades* ❭.
2. Find the upgrade *Initiate SuccessFactors Identity Authentication Service Integration* and click *Learn More & Upgrade Now*.
3. Click *Upgrade Now.*
4. Enter your *S-User* and password in the dialog and click *Validate*.

   We match the information you entered against our records to make sure it's correct. If you enter invalid credentials or you aren't part of the organization who owns the system you're working in, you can't proceed.

5. Select a tenant from your list of displayed tenants or select request a new tenant to the Identity Authentication Service.

   If you're a Partner-Managed Cloud (PMC) customer, you can only request a new tenant.

> ⚠ **Caution**
>
> If your company is already using a productive tenant for Identity Authentication, we strongly recommend that you reuse it and migrate with that productive SAP SuccessFactors tenant. Using one Identity Authentication tenant for your SAP cloud applications is important for other integration scenarios between these applications. Starting with this simplified configuration can help to avoid the need to migrate the integrations and to redesign the landscape. If your company has a specific requirement (functional or legal) where existing Identity Authentication usage or users should not be mixed with the usage and users then, SAP SuccessFactors you can proceed to request an additional Identity Authentication tenant dedicated to SAP SuccessFactors.
>
> We recommend, for test environments, that you have at least one Identity Authentication tenant that is shared with various SAP cloud applications so that you can test a production-like scenario. If you have additional SAP SuccessFactors test instances that cannot be mapped to a test tenant with multiple applications, then you can request a dedicated Identity Authentication tenant for these instances so that they're managed separately.

> **i Note**
>
> The tenants available for upgrade are listed according to the tenants in your region. If the tenant that you want to upgrade is located in a different region or you don't see the tenant that you want to upgrade, please contact customer support so that they can remove the flag that checks your tenant for the region and type.

Upgrade to Initiate SuccessFactors SAP Cloud Platform Identity Authentication Service Integration

ℹ The username and password were successfully validated.

Choose an SAP Cloud Platform Identity Authentication Service tenant from the following options:

🔵 https://gswgzzwnn.ias.ondemand.com
Tenant Type: **test**, Region: US1

⚪ https://yjvgeywfn.ias.ondemand.com
Tenant Type: **test**, Region: US1

⚪ https://gmeycvpue.ias.ondemand.com
Tenant Type: **test**, Region: EU1

⚪ https://gldbtjeum.ias.ondemand.com
Tenant Type: **test**, Region: BR1

[Cancel] [Request New Tenant] [Submit]

6. Click *Yes* to confirm the upgrade and begin the integration process.

Results

The integration process runs in the background and can take up to 24 hours to complete. After the upgrade process completes, an email is sent with tenant details. You can monitor the progress of your upgrade using the identity authentication monitoring tool.

If your organization did not have an Identity Authentication service tenant, we create one during the upgrade process and you're added as its administrator, based on your *S-User* information. You receive an e-mail notification to register your new account.

If you provided the URL of an existing Identity Authentication service tenant, the SAP SuccessFactors system you're working in is added to the Applications section of the Identity Authentication service tenant. You aren't added as a new administrator. Current administrators can go there to complete the configuration.

> ℹ **Note**
>
> The Identity Authentication service is **not** enabled and used by your system yet. You still have to configure it and then turn it on when you're ready.

Setting Up SAP SuccessFactors with Identity Authentication and Identity Provisioning
Services
16   PUBLIC
Getting Started with Identity Authentication and SAP SuccessFactors

Next Steps

After you receive notification that the process completed successfully, review default configuration settings in the Identity Authentication service tenant and confirm that the user sync is functioning properly.

If the upgrade fails for some reason, use the *Undo* option in *Upgrade Center*, within 30 days, to rerun the upgrade after you've resolved the cause of the failure. If you're not sure why the upgrade failed or how to fix it, contact SAP Cloud Support.

> **i** Note
>
> The *Undo* option in *Upgrade Center* only allows you rerun a failed upgrade. It can't undo a successful integration.

Related Information

4.2.1 Monitoring Tool for the Upgrade to SAP Cloud Identity Services - Identity Authentication

When you select to initiate your upgrade to SAP Cloud Identity Services - Identity Authentication service, you're given a link to access the monitoring tool. You can use this tool to see the status of your upgrade and which steps are complete or if an error occurs.

When you initiate your upgrade to the Identity Authentication service, and while the upgrade is processing, you can track the status of your upgrade, using the upgrade monitoring tool. The monitoring tool displays each upgrade task in your upgrade, as it's completed. If an error occurs, the monitoring tool displays the error message and let's you know how to proceed.

> **→** Tip
>
> If you are reusing an Identity Authentication tenant, ensure that you have access to the admin user credentials.

> **i** Note
>
> If an error occurs during the upgrade, take note of the *Upgrade Process ID* so that customer support can identify your issue.

The monitoring keeps track of the following status indicators:

- Validate Customer and Tenant Details
- Set up Identity Authentication Service Tenant

Setting Up SAP SuccessFactors with Identity Authentication and Identity Provisioning
Services
Getting Started with Identity Authentication and SAP SuccessFactors   PUBLIC   **17**

- Configure Identity Authentication Service Tenant
- Set up Identity Provisioning Service Tenant
- Upgrade the Identity Authentication Service Tenant
- Confirmation Emails
- Upgrade Complete

Admin Center / Monitoring Tool for Identity Authentication Service/Identity Provisioning Service Upgrade

Monitoring Tool for Identity Authentication Service/Identity Provisioning Service Upgrade
Initiated on: Feb 20, 2020 10:57AM

| Validate Customer Tenant Details | Set up SAP Cloud Platform Identity... | Configure SAP SuccessFactors... | Set up SAP Cloud Platform Identity... | Configure SAP SuccessFactors... | Send Confirmation Emails |

The upgrade is in progress.
If the problem still persists, please contact customer support.

More Information

Upgrade Process ID: 1712374
Status: In Progress

Identity Authentication Service Tenant URL:
Identity Provisioning Service Tenant URL:

4.3 Setting Up an API User for Sync Jobs in SAP SuccessFactors

The API user created during the upgrade process is called *IPSADMIN*. This user is intended to become your API user after you've given them the listed permissions. The user that you use to log into the Identity Provisioning Administration Service with has separate credentials.

Context

> → Tip
>
> After you receive your Identity Provisioning Service tenant, there are two areas where you must reset passwords:
>
> - reset the password for the IPSADMIN user in your SAP SuccessFactors system
> - reset the password in your Identity Provisioning tenant in the following location: ▷ *Source Systems* ▷ *Properties* ▷ *Password* ▷ *Edit* ▷ *Save* ▷.

Create an allowlist of IP Address ranges so that Identity Authentication API calls are accepted by SAP SuccessFactors. For more details about Country/Region information, refer to the **Regional Availability** topic in the Related Information section below.

Syncing users into the Identity Authentication Service requires that the administrator is granted the necessary role-based permissions. Before proceeding, ensure that your API User has the following permission. For **new** instances, set a password for the **IPSADMIN** user.

Procedure

1. Log on to your SAP SuccessFactors system as `SF Admin`.

2. Go to the *Admin Center*.

3. Select ▶ *Company Settings* ❯ *Password & Login Policy Settings* ◀.

4. Select *API Login Exceptions*.

5. Select *Add*.

6. Enter the *Username* `IPSADMIN`, unless you've created another username.

7. Set *Maximum Password Age* in days to `-1`.

> ⚠ Caution
>
> The password for this user should NOT expire.

8. Enter the following IP address ranges in the *IP address restrictions* field.

Region	Host URL	IP Range
Australia (Sydney)	ap1.hana.ondemand.com	210.80.140.0-210.80.140.255,157.133.96.0-157.133.97.255
Brazil (São Paulo)	br1.hana.ondemand.com	157.133.246.0-157.133.246.255
Canada (Toronto)	ca1.hana.ondemand.com	157.133.54.0-157.133.54.255,157.133.62.0-157.133.62.255
Europe (Amsterdam)	eu3.hana.ondemand.com	157.133.140.0-157.133.140.255,157.133.141.0-157.133.141.255
Europe (Frankfurt)	eu2.hana.ondemand.com	157.133.70.0-157.133.70.255,157.133.204.0-157.133.204.255,157.133.205.0-157.133.205.255,157.133.206.0-157.133.206.255
Europe (Rot)	hana.ondemand.com eu1.hana.ondemand.com	155.56.128.0-155.56.255.255
Japan (Tokyo)	jp1.hana.ondemand.com	157.133.150.0-157.133.150.255
Kingdom of Saudi Arabia (Riyadh)	sa1.hana.ondemand.com	157.133.93.0-157.133.93.255
Russia (Moscow)	ru1.hana.ondemand.com	157.133.2.0-157.133.2.255
UAE (Dubai)	ae1.hana.ondemand.com	157.133.85.0-157.133.85.255

Region	Host URL	IP Range
US East (Ashburn)	us1.hana.ondemand.com	65.221.12.0-65.221.12.255,206.112.73.0-206.112.73.255,157.133.16.0-157.133.16.255,157.133.18.0-157.133.18.255
US West (Chandler)	us2.hana.ondemand.com	64.95.110.0-64.95.110.255,64.95.111.0-64.95.111.255,157.133.24.0-157.133.24.255,157.133.25.0-157.133.25.255,157.133.26.0-157.133.26.255
US East (Sterling)	us3.hana.ondemand.com	169.145.117.0-169.145.117.255,169.145.117.0-169.145.117.255
US West (Colorado Springs)	us4.hana.ondemand.com	157.133.45.0-157.133.45.255
Europe (Rot) - Trial	hanatrial.ondemand.com	155.56.128.0-155.56.255.255

9. Enter the following IP address ranges (for Identity Authentication) in the *IP Address Restrictions* field.

> **i Note**
>
> The Country/Region designation for your administration console is displayed within brackets in the *SAP Identity Authentication Service [Country/Region]* header of your console's web application screen.

Country/Region	IP Range
Australia/Japan	157.133.168.32-157.133.168.63,130.214.240.32-130.214.240.63,157.133.182.32-157.133.182.63,130.214.244.32-130.214.244.63
Brazil	157.133.174.32-157.133.174.63,130.214.236.32-130.214.236.63
China	157.133.168.32-157.133.168.63,130.214.218.32-130.214.218.63
Europe	157.133.160.32-157.133.160.63,130.214.226.32-130.214.226.63,157.133.170.32-157.133.170.63,130.214.230.32-130.214.230.63
Japan	157.133.182.32-157.133.182.63,130.214.244.32-130.214.244.63,157.133.184.32-157.133.184.63,130.214.246.32-130.214.246.63
Canada	52.138.39.15,52.156.1.159,52.138.35.110
Russia	157.133.172.32-157.133.172.63,130.214.252.32-130.214.252.63
Saudi Arabia	130.214.222.32-130.214.222.63
Singapore	18.139.247.210,18.139.185.121,52.76.36.0

Country/Region	IP Range
US/Canada	157.133.166.32-157.133.166.63,130.214.234.32-130.214.234.63,157.133.176.32-157.133.176.63,130.214.238.32-130.214.238.63
US West	51.143.120.222,52.148.160.0,52.143.74.249

10. Save your changes.

11. Grant permissions to your API user (IPSADMIN) that allows them to sync users. At a minimum, give the API user the following role-based permissions:

    ○ ▌ *Manage Integration Tools* ❯ *Allow Admin to Access Odata API* ❯

    ○ ▌ *Manage User* ❯ *User Account OData API Entity* ❯

    ○ ▌ *Manage User* ❯ *Employee Export* ❯

> → Tip
>
> For information about how to give Role-Based Permissions to a user, review the topic linked below: **What Are Role-Based Permissions**.

12. Reset password for the API user (IPSADMIN).

    You only need to reset the password if the user you created is being reused and already existed.

13. In ▌ *Admin Center* ❯ *Manage Employees* ❯.

14. Select *Reset User Passwords*.

15. Go to *Reset Individual User Password* (with supplied password).

16. Enter your username **IPSADMIN**, unless you've created another username.

17. Search **Users**.

18. Select the appropriate user.

19. Enter your new password twice.

20. Choose *Reset User Password*.

> ⚠ Caution
>
> The user performing these steps needs access to **ALL** users in the instance. If your organization assigns separate admins to distinct groups of users, you must ensure that this user has access to all those groups.

Results

You can use this user to configure the *Identity Provisioning Service*.

Related Information

Regional Availability

4.4 Testing and Activating the Upgrade to SAP Cloud Identity Services - Identity Authentication

Test your SAP Cloud Identity Services - Identity Authentication service configuration before activating your migration.

Prerequisites

- You've initiated your Identity Authentication service migration in the *Upgrade Center*.
- You've set up your authentication configurations in the Identity Authentication Service Administration.
- You've set up your source and target configurations in the Identity Provisioning Service Administration.
- You have the corporate identity provider log on information.

> **i Note**
>
> o If you're using a third-party provider, ensure that you have the credentials to log on to the corporate IdP.
>
> o If the Identity Authentication service is your corporate IdP, ensure that you have the login credentials for your Identity Authentication user.

Context

This video references, visually, the steps to test your migration before activating the Identity Authentication Service.

Open this video in a new window

> **! Restriction**
>
> After you've upgraded to the Identity Authentication service, you will not have the ability to turn on partial SSO in SAP SuccessFactors company Provisioning. By default, partial SSO is disabled after activating Identity Authentication. If needed, you can set up partial SSO in Identity Authentication.
>
> After you've upgraded to the Identity Authentication service, you will not have the ability to enable multiple SAML asserting parties in SAP SuccessFactors company Provisioning. By default, Identity Authentication will be enabled as the single SAML asserting party in the SAP SuccessFactors provisioning setting after activating Identity Authentication. If you need multiple asserting parties, you can accomplish this by setting up conditional authentication.

Procedure

1. Log on to your SAP SuccessFactors system as an admin.

2. Go to ▌ *Admin Center* ❯ *Upgrade Center* ❯ *Optional Upgrades* ❯.

3. Find the upgrade *Activate SuccessFactors Identity Authentication Service Integration* and choose *Learn More & Upgrade Now*.

4. Click *Upgrade Now,* on the *Activate SuccessFactors Identity Authentication Service Integration*.

5. Click *Test Now* on the *Test SuccessFactors to Identity Authentication Service Integration* pop up, to test your migration.

   After clicking *Test Now* a new tab opens to your corporate identity provider's log on screen.
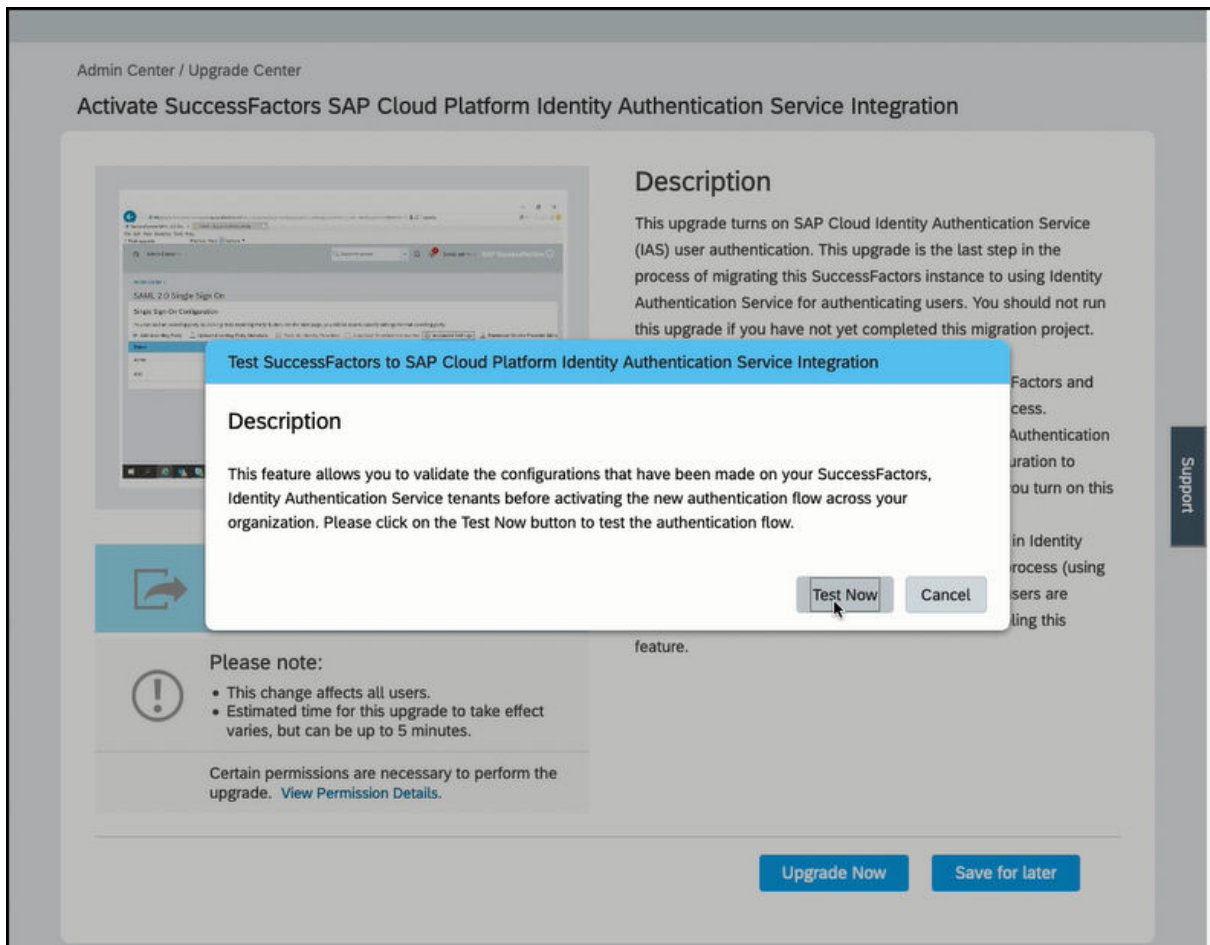
6. Log on to your corporate identity provider based on your corporate IdP scenario.

   ○ If Identity Authentication is your corporate IdP, log on to Identity Authentication using any user's credentials. For a successful test, this user must exist in both Identity Authentication and SAP SuccessFactors.

   ○ If Identity Authentication is being used as a proxy to your corporate IdP, log on to your corporate IdP using your corporate IdP credentials. For a successful test, this user must exist in both Identity Authentication and SAP SuccessFactors.

7. Click *Yes* to activate Identity Authentication.

Setting Up SAP SuccessFactors with Identity Authentication and Identity Provisioning
Services
Getting Started with Identity Authentication and SAP SuccessFactors   PUBLIC   **23**

If your using Onboarding to activate employees, refer to the following topic: **Activating an Account and Setting a New Password After Identity Authentication is Enabled**

Related Information

How to Implement Partial SSO after IAS implementation on SuccessFactors

Activating an Account and Setting New Password After SAP Identity Authentication Service Is Enabled

Configure the Corporate Identity Provider

5 Configure Transformations in SAP Cloud Identity Services - Identity Provisioning

While the default transformations work well when using password-based logins, you may want to further control how data is read and received in Identity Authentication by updating the Identity Provisioning transformations. You can edit transformations to **remove test/dummy emails**, define your **sendmail** settings and to define the **password status** attribute.

When updating your transformations, review both the *Source* and *Target* transformations in the Identity Provisioning console. These transformation areas have different configurations that you can update. Select the application that matches your SAP SuccessFactors instance (Note, for customers with multiple SAP SuccessFactors Instances using the same Identity Authentication. Typically, you will only sync users from one SAP SuccessFactors instance to the Identity Authentication service . No need to import the same people multiple times). Select the Transformations button. This shows you how data gathered from SAP SuccessFactors is transformed while being read into Identity Provisioning service. Typical edits you might make to your source transformations include fixing blank/duplicate emails, setting passwords, setting groups.

> **i Note**
>
> After editing your transformations, run an sync job in the Identity Provisioning service so that your changes are loaded into your integration.

> **→ Tip**
>
> For information about how to configure Identity Provisioning Transformations when you've already migrated to Identity Authentication, review the guide that describes this process: IPS Transformations Document

5.1 Migrating Passwords from SAP SuccessFactors to the SAP Cloud Identity Services - Identity Authentication Service

Configure password migration from your SAP SuccessFactors instance to your Identity Authentication tenant.

Prerequisites

- You've provisioned the users from SAP SuccessFactors to the Identity Authentication service.
- Users provisioned to Identity Authentication have the sourceSystem attribute with value 100, and the sourceSystemId with value equal to the SAP SuccessFactors company ID.

- Configure your IP address ranges for both your Identity Authentication service and Identity Provisioning service. Find the IP address ranges listed in the **Setting Up an API User for Sync Jobs in SAP SuccessFactors** topic. See the Related Information section below.

Context

Configure your SAP SuccessFactors passwords (source system) to integrate with the Identity Authentication service (target system) so that your users will not need to create new passwords once the integration is complete.

Procedure

1. Configure SAP SuccessFactors instance as a password source system in your Identity Authentication tenant as it is described in the **External Source Systems** topic in the Related Information section below.
2. Modify the Identity Provisioning configuration responsible for writing users in Identity Authentication. Go to
   Identity Provisioning Administration > *Target Systems (your Identity Authentication target system configuration)* > *Transformations* tab.
3. In the *Users* > *Mappings* section, include the following elements where `SFCompanyID` is the `SF Company ID` of the integrated instance:

Example

> ⌁ Sample Code

```
{
    "constant": "SFCompanyID",
    "targetPath": "$.sourceSystemId"
},

{
    "constant": "100",
    "targetPath": "$.sourceSystem"
}
```

> → Remember

You also need to update the following elements, so the users don't receive activation emails:

> ⌁ Sample Code

```
{
    "constant": "false",
    "targetPath": "$.sendMail",
    "scope": "createEntity"
```

```
        },
        {
            "constant": "true",
            "targetPath": "$.mailVerified",
            "scope": "createEntity"
        },
        {
            "constant": "enabled",
            "targetPath": "$.passwordStatus",
            "scope": "createEntity"
        },
```

Related Information

Identity Provisioning Transformations
External Source Systems
Setting Up an API User for Sync Jobs in SAP SuccessFactors

5.2 Remove Dummy Emails Transformation

You may want to remove any dummy emails from your system before syncing your users to Identity Authentication and you can do that by adding the following code snippet to your source transformations.

The following code sets email addresses to `username + @sap-test.de`. This guarantees that the email is unique. You are not required to use **sap-test .de**. However, we encourage you to use **sap-test.de**. This test email address does not route to an actual email server. If you use your own email domain, the server will need to reject all the emails.

> ⌨ Sample Code
>
> Find the code block that contains your email transformation and add the dummy email transformation code **underneath** the email transformation.
>
> ```
>     {
>             "sourcePath": "$.email",
>             "targetPath": "$.emails[0].value"
>     },
> ```
>
> The following code looks for emails in the format **no-email@test.com**. Replace this email with your own dummy email addresses. You can add multiple conditions by using the || (OR) operator.
>
> ```
>         {
>             "condition": "($.email == 'no-email@test.com')",
>             "sourcePath": "$.personKeyNav.userAccountNav.username",
>             "targetPath": "$.emails[0].value",
>             "functions": [
>                 {
>                     "type": "concatString",
>                     "suffix": "@sap-test.de"
>                 }
> ```

```
            ]
        }
```

5.3 Define `SendMail` Transformation

Enable the `SendMail` transformation code if you want users receive email notifications when they're created in Identity Authentication.

▤ Sample Code

```
            "constant": "true",
            "targetPath": "$.sendMail",
            "scope": "createEntity"
```

Setting to false prevents the emails from being sent.

▤ Sample Code

```
            "constant": "false",
            "targetPath": "$.sendMail",
            "scope": "createEntity"
```

5.4 Define `PasswordStatus` Transformation

When users first log in with their username and password, when enabled, the Identity Authentication Service does a one-time verification that the password entered matches the existing SAP SuccessFactors Password.

▤ Sample Code

```
            "constant": "enabled",
            "targetPath": "$.passwordStatus",
            "scope": "createEntity"
```

Set to disabled if your users are receiving welcome emails and resetting their passwords before first login.

▤ Sample Code

```
            "constant": "disabled",
            "targetPath": "$.passwordStatus",
            "scope": "createEntity"
```

5.5 Define `PreferredLanguage` Transformation

Use the `PreferredLanguage` transformation code if you want to set the language to be used for the activation email you send to your users.

> 🖥 Sample Code
>
> ```
> {
>             "sourcePath": "$.preferredLanguage",
>             "optional": true,
>             "targetPath": "$.preferredLanguage"
>         },
> ```

Setting the constant to a specific locale is useful if all your activation emails are for only one language.

> 🖥 Sample Code
>
> ```
> {
>             "constant": "es_ES",
>             "targetPath": "$.preferredLanguage"
>         }
> ```

> → Remember
>
> Unless you define another default locale for your company, U.S. English is the default locale for all users. If no translation is present, text appears in the company's default locale.

For more information, refer to the **SAP SuccessFactors Languages and Locales** topic in the *Managing Languages and UI Labels* guide. See the Related Information section below.

Related Information

SAP SuccessFactors Languages and Locales

5.6 Set Up Default Passwords Using Transformations

We recommend that you choose one of the recommended options for assigning an initial password:

- **Option 1**: You can use the password that's initially set up during the user sync in the Identity Provisioning service
- **Option 2**: You can use the SAP SuccessFactors user attribute value as a password
- **Option 3**: You can set an initial password by combining last name with an internal userID, something that only the employee aware of.

Password Set to an SAP SuccessFactors User Attribute

You can use the following transformation configuration to set the initial password to the SF Employee ID attribute.
In the ▶ *Identity Provisioning Administration Console* ❯ *Source Systems* ❯ *Select your Source System* ❯
Transformations ❯.

> ⇶ Sample Code
>
> ❖ Example
>
> In your *Source Systems* Under `User` and `Mappings`, add the following code:

```
        {
         "sourcePath": "$.empId",
         "targetPath": "$['urn:sap:cloud:scim:schemas:extension:sfsf:2.0:User']
['empId']"
        }
```

> ⇶ Sample Code
>
> ❖ Example
>
> In your *Target Systems* Under `User` and `Mappings`, add the following code:

```
        {
         "constant": "false",
         "targetPath": "$.sendMail",
         "scope": "createEntity"
        },
        {
         "constant": "true",
         "targetPath": "$.mailVerified",
         "scope": "createEntity"
        },
        {
         "constant": "initial",
         "targetPath": "$.passwordStatus",
         "scope": "createEntity"
        }
```

```
        {
         "sourcePath": "$['urn:sap:cloud:scim:schemas:extension:sfsf:2.0:User']
['empId']",
         "targetPath": "$.password",
         "scope": "createEntity"
        }
```

> → Tip
>
> You can use a different SAP SuccessFactors user attribute by changing the attribute name `empId` to the name
> of the attribute that you want to use but you must use the name of the attribute as it's defined in the SF OData
> API. Additionally, ensure that this attribute is part of the list in *sf.user.attributes* property.

Password Set by Combining SAP SuccessFactors User Attributes

By default, the Identity Provisioning Service extracts attributes from a subset of SAP SuccessFactors user attributes. These user attributes are listed under the *Properties* tab in the *sf.user.attributes* field. To use additional user attributes, ensure that the needed attributes are included in the *sf.user.attributes* property so that they can be extracted from the SAP SuccessFactors system during user provisioning.

> ⁘ Example
>
> If you'd like to use the *loginMethod* attribute, include the following element in your *Target System* transformation: ▌▶ *Identity Provisioning Administration Console* ❯ *Source Systems* ❯ *Select your Source System* ❯ *Transformations* ▐ Under `User` and `Mappings`, enter the following code:

> ⇆ Sample Code
>
> ```
>         {
>             "sourcePath": "$.loginMethod",
>             "optional": true,
>             "targetPath": "$['urn:sap:cloud:scim:schemas:extension:sfsf:
> 2.0:User']['loginMethod']"
>         }
> ```

5.7   Instance Migration with SSO Login for Corporate Users

Migrate an SAP SuccessFactors Instance where SSO is configured with SAML-based Corporate Identity Provider (IDP).

After migration, users who log in using SSO will be redirected through the SAP Cloud Identity Services - Identity Authentication service tenant to the Corporate IDP to have the same user experience. If there are also password-based log in users (Partial SSO is enabled), they'll start using the Identity Authentication tenant for authentication.

Using the new Identity Authentication solution integrated with SAP SuccessFactors application you can configure delegated authentication to an existing Corporate Identity Provider (using SAML proxy approach). In doing this, the user accesses the SAP SuccessFactors application and will be redirected through the Identity Authentication service to the Corporate IDP, which will provide SSO authentication. Using this method allows you to keep your current user experience but allows you to also benefit from the advanced security features provided by Identity Authentication service, such as 2-factor authentication. Concurrently, you can use the Identity Authentication service tenant for authentication of users that are currently using password-based logins and are **not** part of the corporate environment, such as for partners, third parties, and consultants. In addition, you can configure Risk-Based authentication rules in Identity Authentication, so that under different conditions, access to the SAP SuccessFactors application could be denied, or second factor of authentication could be requested.

5.7.1 Pure SSO Scenario with One Corporate Identity Provider

Setup a SAML trust between your SAP Cloud Identity Services - Identity Authentication service tenant and a corporate Identity provider.

Prerequisites

Establish a trust between the Corporate Identity Providers (IDP) and your Identity Authentication service tenant. Having this trust established, Identity Authentication provides options for delegated authentication (SAML proxy) to one or more corporate identity providers. You can choose between two options:

- **Pure SSO**- All users can access the application using the SAP SuccessFactors application URL (aka SP-Initiated authentication flow)
- **Partial SSO** - Different set of users can use different URLs that point to their specific IDP that redirect to the application after the authentication (aka IdP-Initiated authentication flow)

Procedure

1. Configure the trusted corporate IDP as the default Identity Provider for the SAP SuccessFactors application in Identity Authentication as it is described.

2. Modify the Identity Provisioning configuration responsible for writing users in Identity Authentication. Go to ▶ *Identity Provisioning Administration* ▶ *Target Systems (your Identity Authentication target system configuration)* ▶ *Transformations* ▶ tab.

3. In the ▶ *Users* ▶ *Mappings* ▶ section include the following elements where `SFCompanyID` is the `SF Company ID` of the integrated instance:

   ```
   {
           "constant": "false",
           "targetPath": "$.sendMail",
           "scope": "createEntity"
       },
       {
        "constant": "true",
        "targetPath": "$.mailVerified",
        "scope": "createEntity"
       }
   ```
   ⊨ Sample Code

Related Information

[Configure Trust with Corporate Identity Provider](#)

5.7.2 Partial SSO Login using a Single Corporate Identity Provider

Migrate your SAP SuccessFactors instance when some of your users have SSO-based login and you have external users with SAP SuccessFactors credentials for application access.

At this final step, you should have delegated authentication configured to your Corporate Identity Provider for the SSO-based login users (Corporate Users). While your password-based login users (External Users) use the Identity Authentication service tenant for authentication. You have two options to configure this setup:

As prerequisite for both options you should have established SAML trust between the Identity Authentication tenant and the Corporate IDP.

Option A: Define the Corporate Identity Provider as Default Authentication IDP for the SAP SuccessFactors Application

Using this option, your corporate users can use the SAP SuccessFactors application URL to access the instance. They'll be redirected automatically through Identity Authentication to the Corporate IDP. In addition, your external users can use a special link to Identity Authentication (for IdP-Initiated authentication flow) to login with Identity Authentication credentials and to be redirected to the SAP SuccessFactors application.

Perform the following steps to configure this:

1. Configure the trusted corporate IdP as default Identity Provider for the SAP SuccessFactors application in Identity Authentication as described in the topic Choose Default Identity Provider for an Application.
2. Enable local user authentication in Identity Authentication for SAP SuccessFactors application.

Related Information

Choose Default Identity Provider for an Application

5.8 Group Users Based on Login Method

Using this option, all users (corporate and external) can use the SAP SuccessFactors application URL to access the instance and based on conditional authentication rules some of them (corporate users) will be redirected to the Corporate IDP and others (externals) will authenticate in Identity Authentication with username and password.

Perform the following steps to configure this:

1. Configure in Identity Authentication conditional authentication rules for the SAP SuccessFactors application based on user group, user type or IP-range.
2. (optional) If you wish to use rules, based on user group or user type, modify the Identity Provisioning transformations to ensure that the corporate and external users can have been assigned different user groups or user types.

To differentiate the users in the Identity Provisioning transformation you can use SAP SuccessFactors user attributes, such as *loginMethod* user but you must first ensure that this attribute can be used in the Identity Authentication target system configuration.

During user provisioning, you can assign different user types as listed:

> → Tip
>
> You can use a different SF user attribute by changing the attribute name `empId` to the name of the attribute that you want to use but you must use the name of the attribute as it's defined in the SF OData API. Additionally, ensure that this attribute is part of the list in *sf.user.attributes* property.

The default source SAP SuccessFactors system configuration in Identity Provisioning defines that all users are of type *employee* using the following element:

≡ Sample Code

```
{
            "constant": "employee",
            "targetPath": "$.userType"
        }
```

The following element can be added after the default one in order to overwrite the user type if the *loginMethod* of the user is PWD:

≡ Sample Code

```
{
  "condition": "$.personKeyNav.userAccountNav.loginMethod =='PWD'",
  "constant": "partner",
  "targetPath": "$.userType"
}
,
```

≡ Sample Code

External and Internal users can be assigned to an Identity Authentication user group, which can be used for conditional authentication rules.

> i Note
>
> The user group should exist already in the Identity Authentication tenant.

With the following element added in the Identity Authentication target system configuration in Identity Provisioning, you will have assigned all users with *loginMethod* - `PWD` to a *Password Login Users group*:

≡ Sample Code

```
{
      "condition": "$['urn:sap:cloud:scim:schemas:extension:sfsf:2.0:User']
['loginMethod'] == 'PWD'",
      "constant": "Password Login Users",
      "targetPath": "$.groups[0].value"
    }
```

5.9 Change the Redirect URL for Password Users in Identity Authentication Service

You can change the redirect URL for your users when you update the transformation code in your SAP Cloud Identity Services - Identity Provisioning service.

By default, user provisioning, in the Identity Provisioning service, replicates all SAP SuccessFactors active users in your system. For new users, who are created in SAP SuccessFactors, you must also create them in the Identity Authentication service so that they receive the activation email that will allow them to set a password and to access the SAP SuccessFactors application. With the default configurations to your Identity Provisioning service, any newly created users are redirected to the Identity Authentication service's User Profile page after they activate their account and reset their password. This URL, `https://<customer-tenant-id>.accounts.ondemand.com`, can be customized by adding the following code to your Identity Provisioning's Target System's Transformation.

▶ *Identity Provisioning Administration* ❯ *Target Systems* ❯ *{your Identity Authentication target system configuration}* ❯ *Transformations* ❯ *User Mappings* ❯

In the `User Mappings` section, include the following element:

⌁ Sample Code

```
{
            "constant": "https://custom.domain.net/landing_page",
            "targetPath": "$.targetUrl",
            "scope": "createEntity"
        }
```

In addition to updating the transformation, ensure that the following attributes contain the following values:

- `Target Transformations, $.sendMail attribute` = **True**
- `Target Transformations, $.mailVerified attribute` = **False**
- **Remove** from the Identity Authentication Target System Transformations: `$.passwordStatus attribute`
- Ensure that you add the target URL as a trusted domain in the Identity Authentication Administration console. For more information, review the topic **Configure Trusted Domains**, linked in the Related Information section.

Related Information

[Configure Trusted Domains](#)

6 SAP Cloud Identity Services - Identity Authentication Service Administration Console Tasks

The SAP Cloud Identity Services - Identity Authentication service provides you with secure authentication and single sign-on for users in the cloud.

The Identity Authentication service provides you with simple and secure cloud-based access to business processes, applications, and data. It simplifies your user experience through state-of-the-art authentication mechanisms, secure single sign-on, on-premise integration, and convenient self-service options. The Identity Authentication service functions as both a Service Provider (A resource a user is logging into) and Identity Provider (An Identity Management tool that can authenticate a user and send a logon to a Service Provider).

The Identity Authentication service Administrator system is created when you initiate the upgrade process in the SAP SuccessFactors *Upgrade Center*. As the Identity Authentication Administrator, an email is sent to you with a link to log on to the administration console.

> ⚠ Caution
>
> If you haven't received an email with a link to your identity provisioning system within two hours, contact customer support.

What to Configure in the Identity Authentication Console

The Identity Authentication service gives you access to the following login methods. Configuring these login methods are optional and depends on how you want your users to log into their SAP SuccessFactors systems.

Optional Task	Description	Documentation
Configure password policy settings.	If the default standard password policy doesn't meet your requirements, you can: • Change to the Enterprise password policy • Create a custom password policy For users of two-factor authentication, these password policy settings are still used. For users of single sign-on (SSO) or other nonpassword logon options (like social sign-on), these password policy settings are ignored.	About Password Policies in the Identity Authentication service

Setting Up SAP SuccessFactors with Identity Authentication and Identity Provisioning Services
SAP Cloud Identity Services - Identity Authentication Service Administration Console Tasks

36   PUBLIC

Optional Task	Description	Documentation
Set up single sign-on (SSO).	If you want some or all users to access your system using single sign-on (SSO), you need to set it up. You need to: • Set up trust between the Identity Authentication service and your corporate identity providers. • Set up conditional and/or risk-based authentication rules to determine which users are sent to single sign-on	Process to Set Up Single Sign-On with Identity Authentication [page 42]
Create user groups	If needed, you can set up authentication filtering so that different groups of users are authenticated differently. Create user groups so that you can apply different authentication rules for each group. User groups can be assigned manually or during the user sync with Identity Provisioning service.	About User Groups in the Identity Authentication service
Configure conditional authentication	By default, conditional authentication is configured to send all users to Identity Authentication-based logon. To set up single sign-on, you need to configure conditional authentication rules to send users to your corporate identity provider (IdP).	About Conditional Authentication in the Identity Authentication service
Configure risk-based authentication	By default, risk-based authentication is configured to send all users with Identity Authentication-based logon to username/password logon. You can also configure risk-based authentication rules to send users to two-factor authentication.	About Risk-Based Authentication in the Identity Authentication service
Enable two-factor authentication	If needed, you can choose to enable two-factor authentication as part of your password-based logins.	About Two-Factor Authentication in Identity Authentication service
Configure email templates	You can change the default email templates used to generate email notifications for events such as new users or password reset.	About Email Notification Templates in Identity Authentication service

Optional Task	Description	Documentation
Branding and theming	You can change the default colors and theming used on Identity Authentication pages such as the logon and password reset pages.	About Branding in Identity Authentication

Related Information

Configure the Corporate Identity Provider
SAP Cloud Identity Services - Identity Authentication ↗
Maintaining Conditional Authentication (Video)
Maintaining Risk-Based Authentication (Video)

6.1 Adding Users to the SAP Cloud Identity Services - Identity Authentication Service

As a tenant administrator, you can create a new user in the administration console for Identity Authentication service.

Prerequisites

You're authorized as an admin with the *Manage Users* access in the *Identity Authentication Service*.

> **i Note**
>
> Typically, you'll use the sync job in the Identity Provisioning Administration Console to add users to the system but you can add individual users to the Identity Authentication Service as well.

Procedure

1. Log on to the *Identity Authentication Service* using the link from your registration email.
2. Select *User Management*
3. Select *Add User*.
4. Enter *First Name*, *Last Name*, and *Email Address*.
5. Enter *Login Name*. This log on name must match the exact username of the user in the SAP SuccessFactors, including case.

6. Select the *Employee* as the *User Type*.

7. Select one of the following options:

Option	Description
Send activation e-mail	The user receives an e-mail with instructions how to activate the user account.
Set initial password	The tenant administrator sets the password for the user. i Note The user is prompted to reset the password during the first authentication.

8. Save the changes.

Results

The new admin can access the SAP SuccessFactors instance using Identity Authentication service.

6.2 Creating User Groups in Identity Authentication (Video)

As a tenant administrator, optionally, you can create new user groups in the tenant using the administration console for *Identity Authentication Service*. You may want to do this if you intend to use multiple methods of authentication for your users.

Prerequisites

Your user is authorized with the *Manage Groups* access in the *Identity Authentication Service*.

Context

You may want to create groups and assign users according to the logon method you want each group to use.

Watch the video to learn how and when to create user groups in Identity Authentication.

Open this video in a new window

Procedure

1. Log on to the *Identity Authentication Service*.

2. Select ▌ *Users & Management* ❯ *User Groups* ▌.

3. Select *Add*.

4. Enter *Name*, *Display Name*, and *Description*.

5. Choose *Save*.

6. Manually add a user to one or more groups by selecting *User Management*.

7. Select a user.

   While you can add users to your groups individually, you can add users in bulk using Identity Provisioning Transformations.

8. Select *User Groups*.

9. Choose *Assign Groups*.

10. Select the groups you want to add the user to.

11. Save your changes.

Related Information

Edit Administrator Authorizations
Create a New User Group

6.3 Configure Password Based Logins (Video)

All SAP Cloud Identity Services - Identity Authentication instances are preconfigured with password-based logins by default. If you intend to use password or two-factor logins, review and update your password policy settings.

If the default standard password policy doesn't meet your requirements, you can:

- Change to the enterprise password policy.
- Create a custom password policy.

These settings also apply to two-factor authentication logins.

> **i Note**
>
> If your organization uses single sign-on (SSO) or other nonpassword logon options, such as social sign-on, these password policy settings are ignored.

Watch the video to learn how to configure password policies.

Open this video in a new window

Setting Up SAP SuccessFactors with Identity Authentication and Identity Provisioning
Services
SAP Cloud Identity Services - Identity Authentication Service Administration Console
Tasks

40   PUBLIC

Related Information

Configuring Password Policies

6.4 Configure Two-Factor Authentication

You can set up two-factor authentication if you intend to use multiple layers of authentication for your users.

If you intend to use two-factor authentication, setup password policies and additional two-factor settings. You'll need to sort your users using risk-based authentication and to register their token generator. We support SAP Authenticator, Google Authenticator, and other apps that follow the same standard.

Related Information

About Two-Factor Authentication in Identity Authentication service
About Risk-Based Authentication in the Identity Authentication service
About setting up SAP Authenticator on your phone

6.5 Email Templates and Branding Themes

You can use email templates and branding themes to support your company's themes.

Email Templates

The SAP Cloud Identity Services - Identity Authentication service has email templates for new users, password resets, etc. You'll want to review these and customize to meet your needs. In addition, you'll want to be sure to NOT enable the internal SuccessFactors version of these emails. That includes the Welcome Message when importing new users. There are predefined email templates for user and administrator-related emails. You can also create a custom template set. Unless you have another way to communicate the initial logon URL to your users, we recommend you add a basic logon URL to the New User email.

Themes and Branding

The Identity Authentication service supports basic settings for themes and branding. You can add logos, change colors etc. to the login page and others in Identity Authentication. You will want to review and set them up to meet your needs. SAP Help has more information about Themes and Branding.

Related Information

About Email Notification Templates in Identity Authentication service
About Branding in Identity Authentication

6.6 Process to Set Up Single Sign-On with Identity Authentication

Learn what you need to do to set up single sign-on (SSO) for your SAP SuccessFactors system so that it uses the SAP Cloud Identity Services - Identity Authentication service.

Setting up single sign-on is a multistep process:

1. **Configure your corporate identity provider (IdP).**
   Work with the administrator of your IdP to make the required configurations, using metadata downloaded on the SAP SuccessFactors *SAML 2.0 Single Sign On* page.
2. **Add asserting parties in SAP SuccessFactors.**
   Add your corporate identity provider (IdP) in SAP SuccessFactors as an asserting party to the Identity Authentication service. You can use the SAP SuccessFactors *SAML 2.0 Single Sign On* page or configure it directly in the Identity Authentication administration console.
3. **Configure user groups and authentication rules.**
   Authentication rules determine which user groups use single-sign on and are configured directly in the Identity Authentication administration console.

Related Information

Configure IdP-Initiated SSO

6.6.1 Configuring the Corporate Identity Provider in the Identity Authentication service (Video)

Setting up your corporate IDP in SAP Cloud Identity Services - Identity Authentication service requires that you create a link to your corporate IDP. When you create the IDP, you must also and upload your metadata file so that the metadata exchange occurs between the SAP SuccessFactors Identity Authentication and the company IDP.

Prerequisites

You've received the customer metadata file from your company's Corporate IDP team.

Context

Watch the video or follow the procedure to configure third party Corporate IDP.

[Open this video in a new window](#)

Procedure

1. Log on to the *Identity Authentication Service* using the link from your registration email.
2. Go to *Identity Providers*.
3. Go to *Corporate Identity Providers*.
4. Choose ✚ *Add*.
5. Provide a unique name for your corporate IDP and save your changes.
6. Choose *SAML 2.0 Configuration*.
7. Browse for the metadata from your corporate IDP.

   You should have received the metadata file from your company's corporate identity team.
8. Import the metadata.
9. Select the *SAML 2.0 Compliant* as your identity provider type by clicking *Identity Provider Type* from your *Identity Provider* screen.

   If your provider is ADFS or Azure AD, select *Microsoft ADFS/Azure AD*.
10. Save your changes.

Results

When you've uploaded your metadata file, the fields for *Name* (Issuer), *Single Logout Endpoint* , and *Certificate* are automatically populated.

6.6.1.1 Downloading and Exporting the SAP SuccessFactors Metadata File

The metadata file that you upload should be given to your company's corporate identity provider team in order to complete your identity authentication setup process.

Procedure

1. Log on to the *Identity Authentication Service* using the link from your registration email.
2. Go to *Applications and Resources*.
3. Go to *Tenant Settings*.
4. Go to *SAML 2.0 Configuration*.
5. Select *Download MetaData File* and save the file.
6. Give this file to your corporate identity provider team so that they can import this file into your corporate identity provider. This enables a connection to your IAS.
7. Set up the Identity Provider to send: Name ID Format Unspecified

> **i** Note
>
> The value in the Name ID should match the SAP SuccessFactors Username.

6.7 Implementing Single Sign-On After Upgrading

When you upgrade to Identity Authentication, the flag for partial SSO is disabled, by default. You can use partial SSO by sending users in your system through the Identity Authentication Service.

Context

Procedure

1. Log on to your Identity Authentication console as an Identity Authentication Admin.
2. Select ▶ *Applications & Resources* ❯ *Applications* ❯.
3. Choose your SAP SuccessFactors application.
4. Choose *Conditional Authentication*.

5. Select *Allow users stored in Identity Authentication service to log on* in the *Allow Identity Authentication Users Log On* area.

6. Choose *Save*.

   The setting only appears if, by default you have the Identity Provider (SSO) set up, if you don't have Single Sign-on, you do not need this feature.

   If you are using Authentication Rules, you selected Identity Authentication as the *Default Authenticating Identity Provider* and you must change the *Default Authenticating Identity Provider* your SSO. After you've done this, the section *Allow Identity Authentication Users Log* displays.

7. Choose *Save*.

8. Copy the URL below the checkbox and provide that for your non-SSO users to log in.

   The URL look similar to the following: `https://<IAS tenant URL>/saml2/idp/sso?sp=<SF entity ID>&idp=https://<IAS tenant URL>`

9. If on step 5, you changed the *Default Authenticating Identity Provider* to your SSO, you can change back and the URL will still work.

7 SAP Cloud Identity Services - Identity Provisioning Service Administration Console Tasks

The SAP Cloud Identity Services - Identity Provisioning service allows you to manage the transfer of user data from Source Systems (SAP SuccessFactors) to Target Systems (Identity Authentication service). You can use this service to define how your data is read from the Identity Provisioning service into the Identity Authentication service.

Your Identity Provisioning service system is created when you initiate your upgrade to Identity Authentication, in the SAP SuccessFactors *Upgrade Center* and the identity provisioning administrator receives an email with the link to the *Identity Provisioning Administration* console.

> ⚠ Caution
>
> If you haven't received an email with a link to your identity provisioning system within two hours, contact customer support.

The Identity Provisioning service contains access to your *Source Systems* and *Target Systems* and ensures the synchronization of the entities between the two systems or multiple target systems.

You can configure the required provisioning entities in order to ensure proper synchronization between source and target systems. You can also use proxy systems for indirect connections between a system supported by the Identity Provisioning service and an external application that uses a SCIM 2.0 API to consume identities from the proxy system. For example, you can use Identity Provisioning service as an external consuming application.

Properties help you to customize the way your identities are read from a source system or provisioned to the target one. They can also filter which entities and attributes to be read or skipped during the provisioning job.

For every system supported by the Identity Provisioning service, there's an initial (default) transformation logic that converts the system-specific JSON representation of the entities from/to one common JSON. You can keep the default transformation, or modify the mapping rules to reflect the current setup of entities from your source or target system.

- *Source* – a system, where the company is currently managing the corporate identities
- *Target* – a system that needs to be populated with corporate users and other entities.

What to Configure in the Identity Provisioning Console

After upgrading to the Identity Authentication service in the SAP SuccessFactors *Upgrade Center*, you'll need to perform some configurations in the Identity Provisioning console.

- Review and Edit the Settings Populated During the Upgrade Process.
- Configure Transformations to control how your data is read into the Identity Authentication service.
- Create a password for the API user (IPSADMIN).

> **i Note**
>
> This *IPSADMIN* user is created during the upgrade process. As such, you must create a password for this user and grant them the permissions required to perform integration tasks in your SAP SuccessFactors.

- Run sync jobs.

Related Information

SAP Cloud Identity Services - Identity Provisioning Overview(Video) ↗

7.1 Setting Up the Identity Provisioning Source and Target Systems

Initiating the Identity Authentication upgrade automatically configures most of your Identity Provisioning settings but some settings made need edits to ensure that your connections are properly set and your tests sync runs properly.

Prerequisites

- The Identity Authentication upgrade is complete
- You created a password for the newly created API User: *IPSADMIN*

Context

When you initiate the Identity Authentication upgrade, that process creates and configures your Identity Provisioning *Source* and *Target* systems.

Procedure

1. Log on to your *Identity Provisioning Service* system.
2. Go to *Source Systems*.
3. Select the source that reflects the name of your SAP SuccessFactors instance.
4. Go to *Properties*.
5. Scroll down to *User*. Your exact SAP SuccessFactors instance name is to the right of the API user name. For example, `apiuser@instanceName`

If your instance name is not displayed in the source system that you selected, select a different source system until you find the instance that contains the name of your instance in the *User* field.

6. Enter the password you set for your API user in the *Password* field.

7. Review and edit the types of users you want to sync in the *sf.user.filter* field

> ⚠ Caution
>
> The *sf.user.filter* in the *Identity Provisioning Service Administration Console* under the tabs ▐▶ *Source Systems* ❯ *Properties* ❱, contains place holder values called,
> *'sf_username1_placeholder','sf_username2_placeholder'*. Replacing these place holders with a few users can help you to test user provisioning before performing the sync job that pulls in all of your SAP SuccessFactors users into Identity Authentication. Test your selected users by substituting the place holders with usernames from your SAP SuccessFactors system. After testing and ensuring that user provisioning is working correctly, remove the placeholder users and replace them with the value `Active`. This syncs all the active users in your system.
>
> If you change this filter **AFTER** running the user sync, any users not found using the new filter is deleted from the Identity Authentication Service.

8. Ensure that the value in ▐▶ *Source Systems* ❯ *Details* ❯ *System Name* ❱ **and** the value in ▐▶ *Source* ❯ *Properties* ❯ *User* ❱ contain the same instance name.

9. Go to *Target Systems*.

10. Select the source that reflects the name of your SAP SuccessFactors instance.

11. Ensure that the URL in *Properties* matches the URL to your Identity Authentication Service.

    The URL is listed in the Identity Authentication email you received after upgrading your system.

12. From the *Target System*, in the *Details* tab, ensure that the *Source Systems* value matches the value from the *Source System*, noted in Step 8.

    If the source is not listed, choose *Edit* and select your source from the list.

    > ⚠ Caution
    >
    > Use the dropdown list to check on your source. DO NOT uncheck any existing sources.

13. Save your changes.

Results

If you've reviewed or configured your Identity Authentication settings and you've completed your Identity Provisioning configurations, you can set up your sync jobs as described in the topic: **Running and Scheduling Jobs**

7.2 Running and Scheduling Jobs (User Sync)

When changes occur to your users data, a sync job synchronizes the changes to your system. Run sync jobs to load users into your Identity Authentication service, after editing the transformations (how data reads into the Identity Authentication service), anytime changes occur in your data.

Prerequisites

Ensure that you've performed the tasks in: **Setting up the Identity Provisioning Source and Target System**.

> **i Note**
>
> If you have both SAP SuccessFactors and People Analytics, you'll want to configure both before running the user Re-Sync job.

Context

It's important that you set up user sync so that your users exist in the Identity Authentication service. User sync is critical when using the following services and features:

> **⚠ Caution**
>
> - **Conditional Authentication:** To set up with rules that authenticate based on email, user type, or group.
> - **People Analytics, Internal Career Site and other SAP SuccessFactors product areas:** User identifiers can change between product areas and the Identity Authentication service can only map these identifiers correctly when your users are in Identity Authentication.
> - **Global Assignment & Concurrent Employment:** when users log on from different sources, Identity Authentication needs to convert their identifiers so that Identity Authentication understands them. That only happens when user sync has been done and the users are loaded into Identity Authentication.
> - **Enablement of Partial SSO:** If you intend to user partial sso,your users should exist in Identity Authentication.
> - **Two-factor Authentication:** Your users need to exist in Identity Authentication so that you can take advantage of two-factor security features.

Run a provisioning job manually, or set a time interval for automatic (scheduled) jobs. Also, you can choose whether to run a complete read job or a synchronized one. The sync job reads and provisions only the new and updated entities.

If you have a large user population, this may take a long time. The jobs process is set up with basic transformations that load data for all users fromSAP SuccessFactors to the Identity Authentication tenant. You may want to modify these transformations before running the full reload or *Resync Job*. Common changes include syncing passwords for migrating users and replacing blank or dummy email addresses with unique ones. Once the initial user load is completed, you will need to enable the job to run on a schedule.

Procedure

1. In the *Identity Provisioning Administration Console*, select *Source*.
2. From your *Source Settings*, select *Jobs*.
3. Choose a sync job.

> **→ Tip**
>
> As an admin, you can synchronize the user accounts from SAP SuccessFactors to Identity Provisioning service in real time. Refer to the topic *Synchronizing User Account from SAP SuccessFactors to Identity Provisioning Service in Real Time* in the Related Information section.

In the *Read Job* section you can do three things:

○ **Run Job**: This runs the delta job that finds changed records only.
○ **Schedule**: You can set the run schedule in minutes. If you schedule more than once a day, make the schedule long enough to insure each run completes before another starts.
○ **Pause/Resume**: Use this to stop and start the schedule.

In the *Resync Job* section, you can choose *Run Now* to do a full reload.

> **⚠ Caution**
>
> The **full reload** deletes any users that were previously loaded by this job but are not found in the current data. The **read job** deletes users if there's a change to the *sf.user.filter* setting, as suggested should be done for testing. If you test with one user and then test with another, the first will be deleted. Users manually added to the IAS tenant will never be deleted by the jobs process.

> **→ Tip**
>
> When an employee is terminated or becomes inactive in your SAP SuccessFactors system, you may also need to deactivate the user in the Identity Authentication service. You can deactivate a user by running an on-demand *Resync Job* (full sync) in the Identity Provisioning service. The full sync job keeps your source and target systems synchronized. To run a scheduled sync between your source and target systems, we recommend that you enforce full reads from time to time. To achieve this, you need to set up the following source system property: `ips.full.read.force.count`.
>
> For example, `ips.full.read.force.count=10` results in alternating full reads after every 10 delta reads are performed. This property only impacts scheduled runs; manually triggered runs are ignored.

Related Information

Synchronizing User Account from SAP SuccessFactors to Identity Provisioning Service in Real Time
Manage Full and Delta Read
Manage Jobs and Job Logs

Setting Up SAP SuccessFactors with Identity Authentication and Identity Provisioning Services
SAP Cloud Identity Services - Identity Provisioning Service Administration Console Tasks

50   PUBLIC

8 Single Sign-On for SAP SuccessFactors

Single Sign-On (SSO) is a property of access control of multiple related, but independent software systems. With this property, a user logs in once and gains access to all systems without being prompted to log in to each of them.

Single Sign-on allows users to access your SuccessFactors instance without entering their username and password each time. Instead of manually logging in to the SAP SuccessFactors application, users are authenticated by your Identity Provider (IdP) and then logged into SAP SuccessFactors automatically.

Single Sign-On can be enabled for all users of your system or for a partial subset of users (called "Partial SSO").

Most customers use the SAML 2.0 protocol to set up Single Sign-On for their instance, but we support a number of other SSO options as well.

SAML 2.0

Security Assertion Markup Language (SAML) is an XML-based, open-standard SSO protocol for exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP).

> → Remember
>
> SAML 2.0 is the recommended method of configuring Single Sign-On for SAP SuccessFactors.

8.1 How Does SAML 2.0 Work?

SAML 2.0 is the recommended method of configuring Single Sign-On for SAP SuccessFactors.

How does SAML 2.0 work?

SSO generally takes place between two parties, the identity provider (IdP) and the service provider (SP). The identity provider has information required to authenticate the users and generate SSO logins. The service provider offers a service that is accessible using with SSO.

The SP must be able to accept IdP-generated SSO logins and identify the user who wants to log in. In this case, SAP SuccessFactors is the service provider, or SP. You can use your own IdP to authenticate users and log them into SuccessFactors.
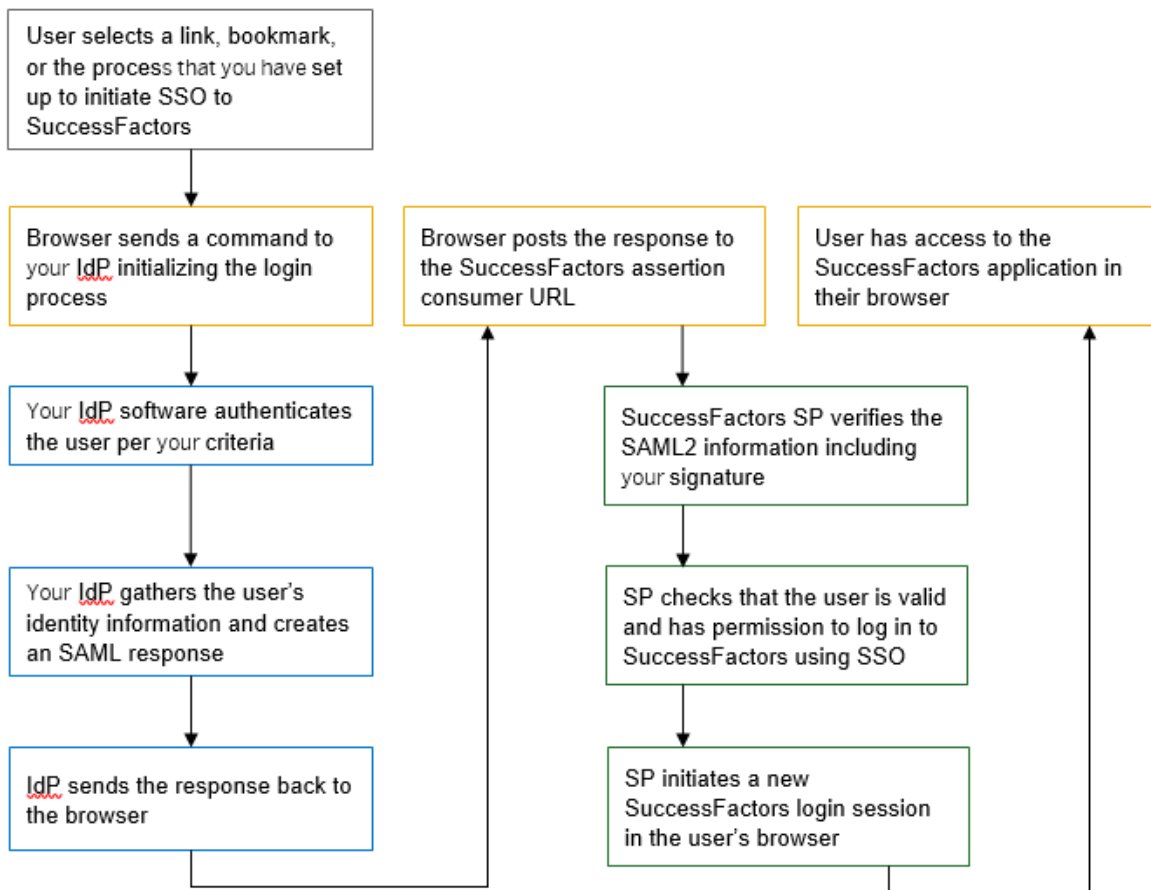
We support the following SAML2 protocols:

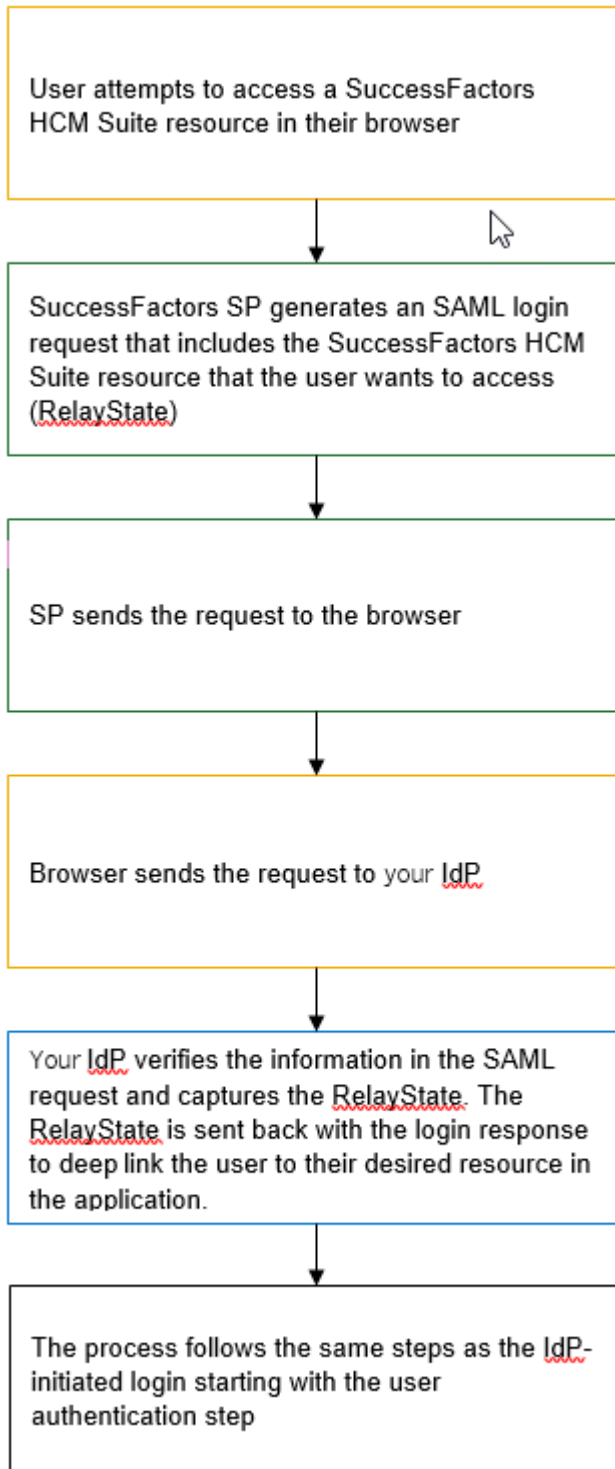- IdP-initiated login, where a user starts the process internally.

- SP-initiated login, where a user starts the process by attempting to connect to SAP SuccessFactors

Here's how these processes work:

Identity Provider (IdP) Initiated SAML Single Sign-On

User selects a link, bookmark, or the process that you have set up to initiate SSO to SuccessFactors

Browser sends a command to your IdP initializing the login process

Your IdP software authenticates the user per your criteria

Your IdP gathers the user's identity information and creates an SAML response

IdP sends the response back to the browser

Browser posts the response to the SuccessFactors assertion consumer URL

SuccessFactors SP verifies the SAML2 information including your signature

SP checks that the user is valid and has permission to log in to SuccessFactors using SSO

SP initiates a new SuccessFactors login session in the user's browser

User has access to the SuccessFactors application in their browser

Service Provider (SP) Initiated SAML Single Sign-On

User attempts to access a SuccessFactors HCM Suite resource in their browser

↓

SuccessFactors SP generates an SAML login request that includes the SuccessFactors HCM Suite resource that the user wants to access (RelayState)

↓

SP sends the request to the browser

↓

Browser sends the request to your IdP.

↓

Your IdP verifies the information in the SAML request and captures the RelayState. The RelayState is sent back with the login response to deep link the user to their desired resource in the application.

↓

The process follows the same steps as the IdP-initiated login starting with the user authentication step

Setting Up SAP SuccessFactors with Identity Authentication and Identity Provisioning Services
Single Sign-On for SAP SuccessFactors

PUBLIC **53**

8.2 SAP SuccessFactors Implementation of SAML 2.0

The SAML2 specification provides a general framework to ensure SAML identity providers (IdP) and service providers (SP) work together properly. Within that framework, service providers offer features that best support their application and their customers. SAP SuccessFactors offers the following:

IdP and SP Logins

You can connect using either or both. The default setup is for IdP-initiated and this must be completed for all SSO customers. Additional settings need to be configured to allow the optional SP-initiated logins.

Dynamic Deep Linking

The SP-initiated login option is designed to allow users to deep link to some place other than the default landing page after an SSO login. For example, the SAP SuccessFactors application typically sends users to our home page. With deep linking, they can land on their performance review or a course in SAP SuccessFactors Learning or countless other locations within the application. When a user is not logged in and tries to access SAP SuccessFactors, we send an SAML request to your identity provider URL. The response contains the login information and landing page details in an additional value called RelayState.

If you do not support SP-initiated SAML2, we offer a generic deep link feature. This accomplishes the same result (deep linking) as SP logins, but uses cookies. When a user is not logged in and tries to accessSAP SuccessFactors, we send their browser to the IdP-initializing URL that you provided. This is typically the same URL that users use to log in directly from their internal systems. The user goes through the IDP-initiated login process. After they are logged in, we read a cookie that was stored with their initial destination, and place them there instead of on the home page.

If you have both deep linking and SP-initiated logins enabled from a single IdP, we use SP-initiated rather than deep linking.

Dynamic deep linking should work with all links sent out by the application itself. These include things sent in system emails, course links generated by SAP SuccessFactors Learning administrators, exported JAM links, and so on. We do not recommend copying the URLs directly from the browser and using them for bookmarks. There is no guarantee that a URL in the browser will create a valid link, or that a link will be valid in the future.

Static Deep Linking

If you use IdP-initiated logins, you can provide us with a RelayState value to send users somewhere other than the home page. We provide a list of supported RelayState values if you plan to use this option.

SP-Initiated Single Logout

You may want to perform some action in your home system when a user logs out of SAP SuccessFactors. If you provide us with the destination URL, we can send a logout request when a user ends a SAP SuccessFactors session.

Multiple Asserting Parties

If you have multiple identity providers, we can set up asserting parties for each one. This includes separate values for SAML issuer, signing certificate, and other settings. If one or more of the asserting parties is set to use SP-initiated logins, one of them can be set to be the default asserting party.

If you have multiple asserting parties and use deep linking, we need to identify to which IdP to send users for login information. If you have a default asserting party, we send them to that IdP. If not, we display a list of the available asserting parties and ask the user to select the appropriate one. Your administrator can configure the text identifying each available asserting party. After a user has logged on using a specific asserting party, we store a cookie in their browser. As long as they use the same browser and don't clear their cookies, they don't need to select the asserting party again.

SSO Redirects

By default, the SAP SuccessFactors application shows users the login page when they log out, time out, or when they get a login error. You can host your own pages for these use cases. If you provide us with the URL or each page, we configure our SSO system to send the users there instead of the home page. We can redirect for the following use cases:

Use Case	Description
Logout	When the user logs out, we send them to the customer-hosted page.
Timeout	After a 30-minute inactivity timeout, we send the user to this page.
Invalid login	If the SSO login fails, we send the user to this page.
Invalid manager	The SAP SuccessFactors HXM Suite application requires a valid manager hierarchy. If it is broken, we send the user to this page.
Missing credentials	If the SAP SuccessFactors application receives an SSO login with no user information, we send the user to this page.
Deep link	Your IdP login link goes here if you plan to deep link, but are not using SP-initiated SAML.

Partial Organization SSO

You can allow some users to use SSO while others log in with passwords. No single user can have access to both methods at the same time. We can provide a document detailing the steps to set up partial SSO.

SAML SSO users do not have access to the password management system and are never forced to change their passwords. Passwords are not used as part of the SAML login process.

Users logging in with passwords are subject to all the password management rules and features that you have enabled.

8.3   SAP SuccessFactors SAML 2.0 Technical Details

The SAP SuccessFactors service provider is configured to accept a wide variety of SAML responses and assertions. However, your IdP must adhere to the following rules:

HTTPS Encryption and POST

All communication with the SAP SuccessFactors application must use HTTPS in the browser. SAML responses sent to SAP SuccessFactors must use POST. URLs sent to deep link into the application and SAML requests do not need to be POSTed.

User Identifier

SAP SuccessFactors accepts two values to identify the user logging in using SAML2. The most common is NameID. We also support the UserName attribute. Whichever method is used, the value is compared with the UserName in the SAP SuccessFactors application. If that user does not exist or does not have permission to log in, the user is unable to access the application.

The system checks for the UserName attribute first. In the assertion, the SAP SuccessFactors application expects something similar to the following:

⇱ Sample Code

```
<saml:AttributeStatement xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<saml:Attribute Name="username"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
<saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string"> lhadley</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

If the UserName attribute is not found, the SAP SuccessFactors application looks for the NameID value. In the assertion, theSAP SuccessFactors application expects something like the following:

⇱ Sample Code

```
<Subject><NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified">lhadley</NameID><SubjectConfirmation
```

```
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><SubjectConfirmationData
InResponseTo="_f6e21384-e33b-4a5f-a532-e58ce3f0a5e2"
NotOnOrAfter="2014-10-21T16:30:56.599Z" Recipient="https://
performancemanager4.successfactors.com/saml2/SAMLAssertionConsumer?
company=TestCompany"/></SubjectConfirmation></Subject>
```

Notice that in addition to NameID, there is nameid-format: unspecified. SAP SuccessFactors expects a nameid-format. Typically, you send the value unspecified. SAP SuccessFactors accepts other common values like persistent or transient. However, there is no support for these other options. Irrespective of the nameid-format sent, SAP SuccessFactors simply compares the NameID from the login to the username in the application. The only exception is the UserName attribute that is sent. In that case, the NameID is ignored entirely.

Certificates and Signatures

SAP SuccessFactors expects the SAML logins to be signed by your certificate. The signature can be on the response, assertion, or both. To verify the signature, you need to provide SAP SuccessFactors with your X509 signing certificate. SAP SuccessFactors accepts both CA and self-signed certificates.

SAP SuccessFactors provides an X.509 certificate for you to encrypt assertion elements if desired. The same certificate is used to sign SP-initiated logout requests.

If you use SP-initiated logins, we provide the X.509 certificate used to sign the SAML login requests.

IP Address Restrictions

SAP SuccessFactors allows you to restrict logins to specific IP addresses or ranges. This feature does not require SSO. However, it applies to SSO logins if SSO is enabled.

Information Exchanged to Set Up SAML2

SAP SuccessFactors supplies you with a setup sheet containing the values that you need and requesting the values that theSAP SuccessFactors application needs. SAP SuccessFactors can also provide and receive metadata files. SAP SuccessFactors does not provide an automated exchange of metadata files.

SAP SuccessFactors provides:

• X.509 certificate that you can use to encrypt assertion values

• SAP SuccessFactors entity ID values

The SAP SuccessFactors entity ID is unique for each SAP SuccessFactors customer instance.

• Assertion consumer service URL

This URL is unique for each SAP SuccessFactors customer instance.

• Global logout response handler URL

This URL is unique for each SAP SuccessFactors customer instance.

You provide:

• X.509 certificate used to sign the response or assertion

• SAML issuer or IdP entity ID

• If you are using IdP-initiated logout, SAP SuccessFactors needs your global logout service URL

• If you are enabling IP address restrictions, SAP SuccessFactors needs the list of IPs

• If you are using the SAP SuccessFactors redirect pages (highly recommended), SAP SuccessFactors needs the URL for each

Timestamps and Server Synchronization

SAML2 requires you to send and SAP SuccessFactors to respect NotBefore and NotAfter values that define when a login is valid. These values are always sent in GMT/UTC. SAP SuccessFactors syncs server time to public time servers on a regular basis. You are expected to do the same. However, there still may be slight variances in the clocks. SAP SuccessFactors asks you to allow a small window of NotBefore time to prevent login failures if server time gets slightly out of sync.

RelayState

If you use IdP-initiated logins, you can specify a RelayState value to deep link your users to a specific page in the application. RelayState is optional. SAP SuccessFactors can provide a list of valid RelayState values. If the deep link value has been populated with your URL, and a user tries to deep link into the application, they go to the destination they expect rather than the RelayState. If SP-initiated logins are enabled, you send SAP SuccessFactors a dynamic value in the RelayState. This takes precedence over the non-sp deep link process.

8.4   Example of Typical Login Response (Decoded)

SAP SuccessFactors accepts a wide variety of formats and values in the SAML2 response. The following is a typical example. Your provided responses may differ.

> ⌨ Sample Code
>
> ```
> <samlp:Response ID="gf8b65pFRW3JOvrV9z8_fjCJJtO"
>     IssueInstant="2009-02-09T11:52:09.484Z" Version="2.0"
>     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
> xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
>     xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
>     <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
> idp1.test.org</saml:Issuer>
>     <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
>         <ds:SignedInfo>
>             <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
> exc-c14n#" />
> ```

```
              <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1" />
              <ds:Reference URI="#gf8b65pFRW3JOvrV9z8_fjCJJtO">
                  <ds:Transforms>
                      <ds:Transform
                          Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
                      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#">
                          <ec:InclusiveNamespaces PrefixList="ds saml samlp xs xsi"
                              xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
                      </ds:Transform>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#sha1" />
                  <ds:DigestValue>8crrNj4pAptpLQKlAzbsS37tfOI=
                  </ds:DigestValue>
              </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>
              bdmIryj5+K9tGsK7sO89j0UwBNQDRee8XpF/
aDY61ERrazaIC1NFwfXN6ETdz61gU5EKY5tJkaHR

YjYTTr8NG1JwSj8JCGePoabuh3KbjgNuE21nQ8JY0TcttPZGMysD4NOzkLIGOTKARp2BUVx7COJC
              egN9yX+SNphxlWD2vMQ=</ds:SignatureValue>
      </ds:Signature>
      <samlp:Status xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
          <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"
              xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" />
      </samlp:Status>
      <saml:Assertion ID="xv5BP-.Sl_aNbpsNwMX259HTgxL"
          IssueInstant="2009-02-09T11:52:09.500Z" Version="2.0"
          xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
          <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:
2.0:assertion">idp1.test.org
          </saml:Issuer>
          <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
              <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified"
                  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"> lhadley</
saml:NameID>
              <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:
2.0:cm:bearer"
                  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                  <saml:SubjectConfirmationData
                      InResponseTo="_F499B815F2BA7AB15F1207741929643"
NotOnOrAfter="2010-04-09T11:57:09.515Z"
                      Recipient=" https://performancemanager.successfactors.com /
saml2/SAMLAssertionConsumer" />
              </saml:SubjectConfirmation>
          </saml:Subject>
          <saml:Conditions NotBefore="2009-02-09T11:47:09.500Z"
              NotOnOrAfter="2009-12-09T11:57:09.500Z"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
              <saml:AudienceRestriction xmlns:saml="urn:oasis:names:tc:SAML:
2.0:assertion">
                  <saml:Audience>https://www.successfactors.com
                  </saml:Audience>
              </saml:AudienceRestriction>
          </saml:Conditions>
          <saml:AuthnStatement AuthnInstant="2009-02-09T11:52:09.500Z"
              SessionIndex="xv5BP-.Sl_aNbpsNwMX259HTgxL"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
              <saml:AuthnContext xmlns:saml="urn:oasis:names:tc:SAML:
2.0:assertion">
                  <saml:AuthnContextClassRef>
                      urn:oasis:names:tc:SAML:2.0:ac:classes:Password
```

```
                </saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement xmlns:saml="urn:oasis:names:tc:SAML:
2.0:assertion"
            xmlns:xs="http://www.w3.org/2001/XMLSchema">
            <saml:Attribute Name="password"
                NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
                    xsi:type="xs:string"> lhadley</saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

9 Configure Single Sign-On in Admin Center

9.1 Opening the SAP Cloud Identity Services - Identity Authentication Administration Console

Navigate from the SAP SuccessFactors *SAML 2.0 Single Sign On* page to the Identity Authentication administration console so that you can configure advanced SAML SSO settings.

Prerequisites

- You have an Identity Authentication service tenant and SAML trust is set up between it and your SAP SuccessFactors system.
- You have the *Manage SAML SSO Settings* permission.

Procedure

1. Go to ▌ *Admin Center* ❯ *Tools* ❯ *SAML 2.0 Single Sign On* ❯.
2. Click *Advanced Settings*.

Results

The Identity Authentication administration console opens in a new tab in your browser.

Related Information

Default Configuration of Identity Authentication Service with SAP SuccessFactors [page 13]
Opening the SAP Cloud Identity Services - Identity Authentication Administration Console [page 61]
More about SAP Cloud Identity Services - Identity Authentication Service

9.1.1 Configure Your Corporate Identity Provider

Configure your corporate identity provider with service provider metadata from the SAP Cloud Identity Services - Identity Authentication service.

Prerequisites

- Your SAP SuccessFactors system is connected to the Identity Authentication service.
- You have the *Manage SAML SSO Settings* permission.

Context

This is the first step in the process of setting up single sign-on for SAP SuccessFactors with Identity Authentication service. In this step, you are setting up Identity Authentication as the service provider that is configured in your corporate identity provider. Configuration is done by the administrator of your corporate identity provider.

About Corporate Identity Providers in the Identity Authentication service

Procedure

1. Download service provider metadata for your Identity Authentication tenant:
   a. Go to ▷ *Admin Center* ❭ *Manage SAML SSO Settings* ❭.
   b. Click *Download Service Provider Metadata*.
2. Register Identity Authentication service as a service provider for your corporate identity provider.

   > → Tip
   >
   > For information about how to do this, consult documentation of your corporate identity provider.

3. (Optional) If you are using IdP-initiated SSO, add the `sp=<sp_name>` parameter to the assertion consumer service (ACS) endpoint URL in your corporate identity provider, replacing the `sp_name` with the `Entity ID` of your Identity Authentication service tenant.

   This parameter is needed for Identity Authentication to know where to redirect the user to after successful authentication.

   > → Tip
   >
   > The ACS endpoint URL should have the following format: `https://<the current ACS endpoint URL>?sp=<sp_name>`.
   >
   > How to request the Entity ID of the service provider from the tenant administrator of Identity Authentication.

4. Configure your corporate identity provider to send the `Name-ID` and `NameIDFormat` that are expected by SAP SuccessFactors:

   `Name-ID`: username

   `NameIDFormat`: unspecified

   > **i Note**
   >
   > If it is not possible to send this information to SAP SuccessFactors and the attributes should be modified by Identity Authentication, you should enable *Identity Federation*.
   >
   > More about Identity Federation.

Next Steps

Proceed to add your corporate identity provider (IdP) as an asserting party to the Identity Authentication service.

9.1.2 Adding an Asserting Party

Add your corporate identity provider (IdP) as an asserting party to the SAP Cloud Identity Services - Identity Authentication service.

Prerequisites

- You have the *Manage SAML SSO Settings* permission.
- You have configured your corporate identity provider with service provider metadata from the Identity Authentication service.
- You have SAML metadata for your corporate identity provider. If you do not have this, contact the administrator of your corporate identity provider.

Context

This is a necessary step in the process of setting up single sign-on for SAP SuccessFactors with the Identity Authentication service. In this step, your corporate identity provider is the asserting party that is configured in Identity Authentication.

We recommend using the *SAML 2.0 Single Sign On* tool to simplify this task and focus on the fields that are required by SAP SuccessFactors. But you can also complete the same task directly in the Identity Authentication administration console.

Procedure

1. Go to ▌ *Admin Center* ❯ *Tools* ❯ *Manage SAML SSO Settings* ❯.
2. Click *Add Asserting Party*.

> **! Restriction**
>
> It is important that Identity Authentication is the **only** SAML asserting party that is enabled after you've activated your upgrade to Identity Authentication. If you add more than one asserting party, that's not Identity Authentication, we recommend that you do **not** enable it. If you enable multiple asserting parties, you will not be able to upgrade to People Analytics.

3. In the *Base Configuration Settings* section, provide the following information.

Field	Description
SAML Asserting Party Name	Enter a name to identify the asserting party. It cannot be modified later.
SAML Issuer	Enter the name of the SAML issuer.
	Extract this from the SAML metadata file provided by the administrator of your corporate identity provider. It is contained in the element `entityID` in the xml file.
SAML Verifying Certificate	Enter the Identity Authentication service IdP signing certificate.
	First, extract this from the SAML metadata file provided by the administrator of your corporate identity provider. The certificate is contained in the following element in the xml file: `IDPSSODescriptor -> KeyDescriptor -> KeyInfo -> X509Data -> X509Certificate`. Then, add the following before and after the certificate:
	Above the copied text: **- - - - -BEGIN CERTIFICATE- - - - -**
	Below the copied text: **- - - - -END CERTIFICATE- - - - -**
Single Sign On Endpoint	Enter the service provider's endpoint URL that receives the response with the SAML assertion from Identity Authentication.
Default Issuer	Set to *Yes* if this Asserting Party is the default Identity Provider. If so, all SP-initiated logins (deep links) will be handled by this IdP.
Global Logout Service URL (LogoutRequest destination)	Enter the Identity Provider's URL that will receive SAML Logout Requests.

64 PUBLIC

Setting Up SAP SuccessFactors with Identity Authentication and Identity Provisioning Services
Configure Single Sign-On in Admin Center

Field	Description
SAML Signing Algorithm	Set the digest algorithm for signing outgoing messages to the following: ○ *SHA-256* - this is the default hashing algorithm for signing certificates for all integrations. *SHA-1* is **not** recommended as *SHA-256* provides a higher level of security.

4. In the *Enable Additional Settings* section, provide the following information.

Field	Description
Redirect URL when logout	Select the checkbox and enter the URL of the page users should see when they log out.
Redirect URL when session timeout	Select the checkbox and enter the URL of the page users should see when the session times out.
Redirect URL for Invalid Login	Select the checkbox and enter the URL of the page users should see when they have a login failure.
Redirect URL for Invalid Manager	Select the checkbox and enter the URL of the page users should see when they have a login failure due to an issue with their manager assignment.

5. Click *Done* to save your changes.

Next Steps

Configure user groups and authentication rules in the Identity Authentication administration console to determine which users are sent to single-sign on.

If you choose, you can also configure additional SSO configuration options.

Related Information

9.1.2.1 Uploading Asserting Party

You can use the *Admin Center* to set up your IDP.

Procedure

1. Go to the *Admin Center*.
2. Search for **Manage SAML SSO Settings**.
3. Select *Upload Asserting Party Metadata*.
4. Enter a name and select the metadata file from your Corporate Identity Provider.
5. Choose *Upload*.

Related Information

Configure Your Corporate Identity Provider [page 62]

9.1.3 Additional Single Sign-On Configurations

Additional single sign-on options can be configured in the SAP Cloud Identity Services - Identity Authentication administration console.

Here are some common use cases and links to relevant documentation.

Use Case	Documentation
Set up authentication rules for sending users to corporate IdP or for multiple asserting party selection.	Conditional Authentication
Set up authentication rules for sending users to two-factor/token authentication, password-based login, or other login options.	Risk Based Authentication
Have the Identity Authentication service send a different value to SAP SuccessFactors than it used to authenticate the user. For example, Identity Authentication can contain a login using an email address but send SAP SuccessFactors the login name for that user.	Name ID Settings
Add asserting parties using Metadata Import in the Identity Authentication Administration Console, instead of using the SAP SuccessFactors *SAML 2.0 Single Sign On* page.	Configure Trust with Corporate IdP

Related Information

9.2 Single Sign-On without SAP Cloud Identity Services - Identity Authentication

To configure single sign-on **without** SAP Cloud Identity Services - Identity Authentication, using other authentication services or identity providers or using non-SAML methods, use the Provisioning application.

> → Remember
>
> As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner. If you're no longer working with an implementation partner, contact SAP Support.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon ![icon] : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:

    - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
    - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.

- Links with the icon ![icon] : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

THE BEST RUN **SAP**